Protection des workloads cloud

Sécurisez les hôtes, les containers et les fonctions sans serveur tout au long du cycle de vie des applications

Hôtes, containers, systèmes Kubernetes®, fonctions sans serveur, environnements d'exécution… Prisma™ Cloud assure une protection des workloads cloud-native tout au long des phases de développement, de déploiement et d'exécution des applications, combinée à une gestion des vulnérabilités et de la conformité.

Classé nº 1 par IT Central Station pour la sécurité des workloads cloud	Classé nº 1 par IT Central Station pour la sécurité des containers	Adopté par plus de 40 % des entreprises du Fortune 100
Protège les workloads des environnements hybrides et multi-cloud	Protège les containers Linux et Windows s'exécutant sur Kubernetes ou d'autres plate-formes	Protège plus de 1 800 clients dans le monde, dont plusieurs entre-prises leaders

Protection unifiée des architec-tures cloud-native

Machines virtuelles (VM), containers et services Kubernetes, PaaS (Platform as a Service), fonctions sans serveur… les entreprises utilisent un mélange de technologies pour exé-cuter leurs workloads et applications cloud. Prisma Cloud s'appuie sur un framework unifié d'agents pour sécuriser tous ces workloads et architectures.

Sécurité intégrée tout au long du cycle applicatif

Prisma Cloud intègre des fonctionnalités de protection des workloads cloud tout au long du cycle de vie des applica-tions. Intégration de la gestion des vulnérabilités et de la conformité aux workflows d'intégration et de déploiement continus (CI/CD) ; surveillance continue des registres de containers et des référentiels sans serveur ; priorisation des risques pendant la phase d'exécution (hôtes, containers et images, fonctions sans serveur)… les avantages sont multi-ples pour les entreprises.

Modules

Sécurité des hôtes

Prisma Cloud Host Security protège les hôtes Linux et Windows® qui s'exécutent dans des clouds publics ou privés. Au menu :

- **Gestion des vulnérabilités** – Recherchez en permanence les éventuelles vulnérabilités sur les hôtes. Les risques sont traités par priorité à l'aide de listes des 10 principales vulnérabilités.
- **Conformité** – Appliquez des contrôles prédéfinis de conformité des politiques de sécurité au moyen du CIS Benchmark pour Linux et de contrôles de configuration Windows, ou mettez en place des contrôles de conformité personnalisés.
- **Sécurité des environnements d'exécution** – Profilez automatiquement le comportement des workloads pour signaler ou bloquer les activités inhabituelles et mal-veillantes. La protection intégrée comprend les modifi-cations (lecture/écriture) sur les fichiers et répertoires, l'inspection des journaux de l'hôte et la création de règles d'exécution personnalisées.
- **Visibilité sur le réseau** – Bénéficiez d'une vue en temps réel sur toutes les communications réseau des hôtes.
- **Contrôle des accès** – Établissez et surveillez les contrôles d'accès associés aux workloads cloud.
- **Analyse des AMI (Amazon Machine Image)** – Recher-chez les vulnérabilités sur les AMI avant de déployer des machines virtuelles sur Amazon Web Services (AWS®).

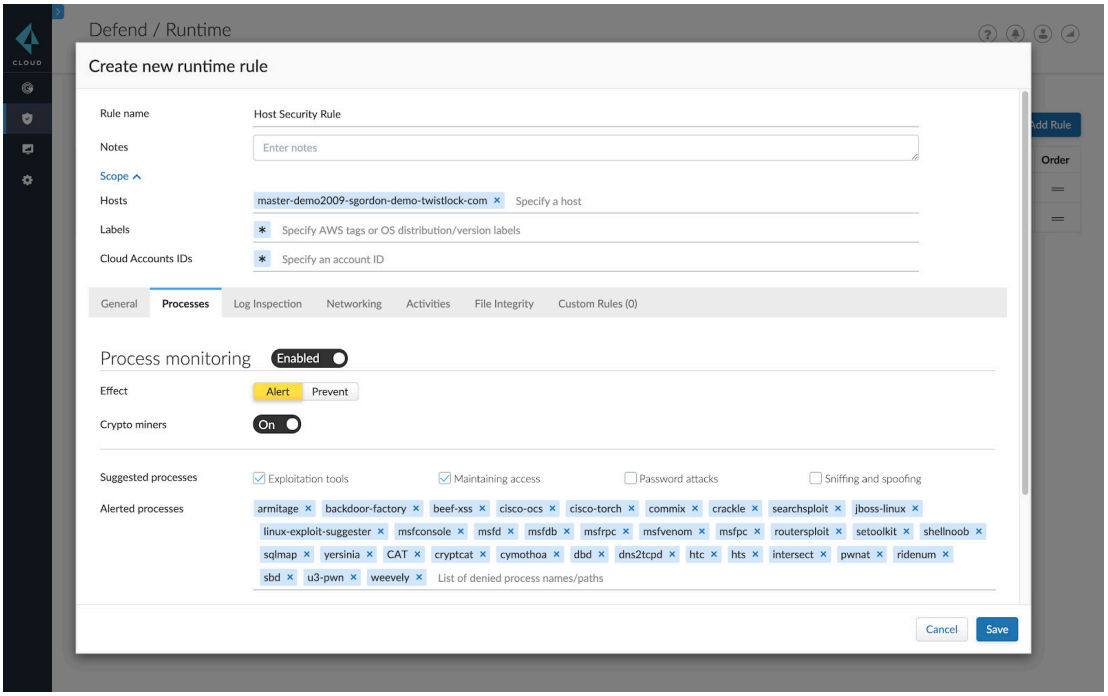

Figure 1 : Sécurité des hôtes

Sécurité des containers

Prisma Cloud Container Security protège les containers et les systèmes Kubernetes qui s'exécutent dans des clouds publics ou privés. Au menu :

- **Gestion des vulnérabilités** – Affichez des informations précises sur les vulnérabilités des images et des containers. Les listes des 10 principales vulnérabilités permettent de prioriser les risques dans toutes les CVE connues. Elles s'accompagnent de conseils de remédiation et d'une analyse des images par couche.
- **Contrôles de conformité** – Exploitez plus de 400 contrôles de conformité (CIS Benchmarks pour Docker®, Kubernetes, Linux, configurations Windows, Istio®, etc.). Les frameworks pré-intégrés et personnalisables respectent les normes en vigueur (PCI DSS, HIPAA, RGPD, etc.) et les spécifications NIST SP 800-190.
- **Sécurité des environnements d'exécution** – Automatisez la création des règles d'exécution au niveau des processus, du réseau et des capteurs de système de fichiers pour protéger les applications en cours d'exécution et assurer leur sécurité au fur et à mesure de leur évolution. Des règles d'exécution puissantes et personnalisées renforcent la sécurité de vos applications containerisées.
- **Visibilité sur le réseau** – Bénéficiez d'une vue en temps réel sur toutes les communications réseau des containers et des systèmes Kubernetes.
- **Contrôle des accès** – Instaurez des mesures de contrôle d'accès pour les applications cloud-native à travers tous les types d'hôtes sous-jacents et les environnements Docker et Kubernetes. Vous pouvez également intégrer la solution à votre dispositif IAM (gestion des identités et des accès), à vos outils de gestion des secrets et à d'autres technologies critiques.
- **Sécurité CI/CD** – Intégrez la sécurité aux workflows CI/CD. Définissez des seuils de vulnérabilité granulaires pour signaler/bloquer des images vulnérables, ou déclencher des alertes/appliquer des politiques de conformité.

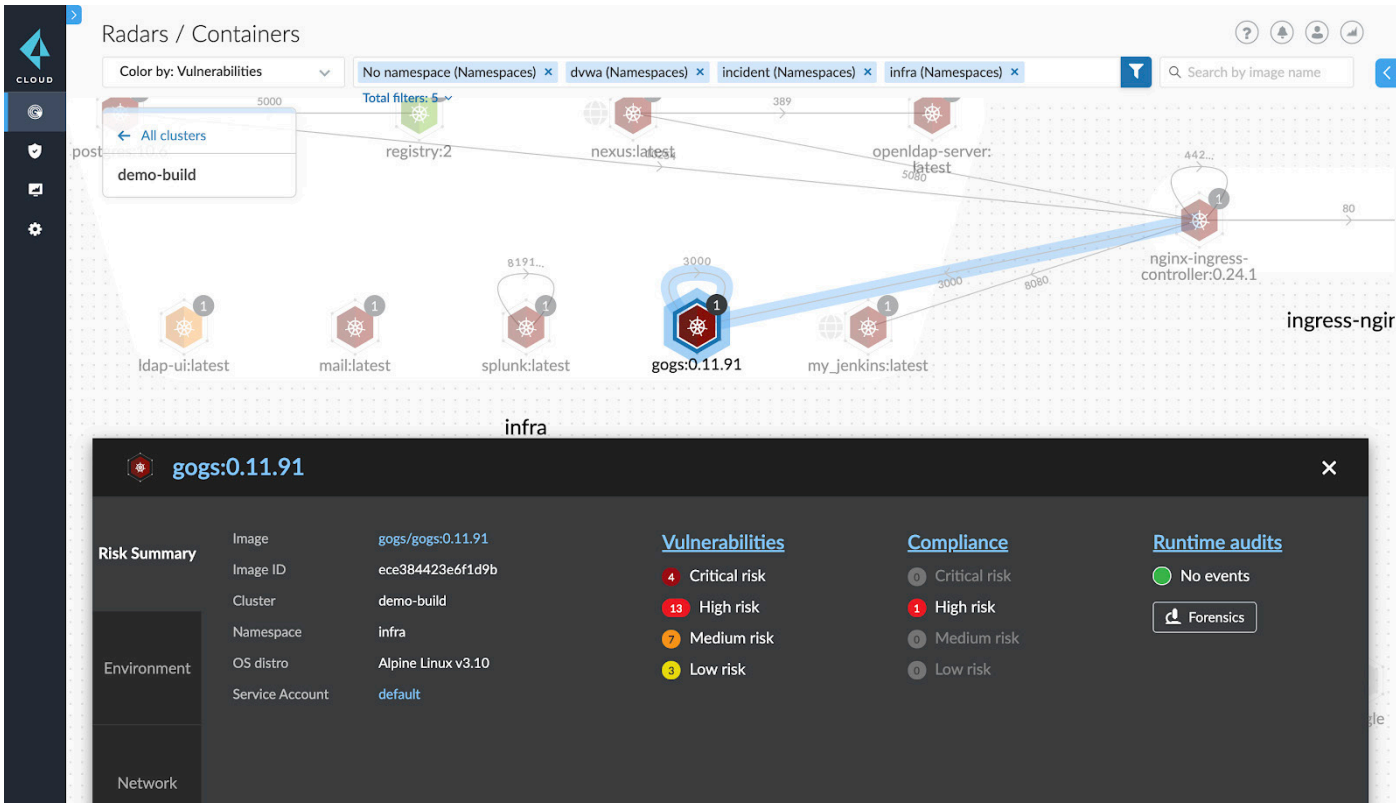

Figure 2 : Sécurité des containers

Sécurité des systèmes sans serveur

Prisma Cloud Serverless Security protège les fonctions sans serveur tout au long du cycle de vie des applications. Au menu :

- **Gestion des vulnérabilités** – Analysez et surveillez en continu les vulnérabilités sur les fonctions, à commencer par les outils CI intégrés et les référentiels sans serveur, et jusqu'à la phase d'exécution pour une vue complète sur les risques associés aux ressources sans serveur.
- **Contrôles de conformité** – Identifiez les erreurs de configuration (clés privées stockées dans des archives zips, accès étendus aux ressources, etc.) pour les équipes DevOps et de sécurité.
- **Sécurité des environnements d'exécution** – Affichez en temps réel dans Radar les fonctions en cours d'exécution sur AWS Lambda : vue sur les déclencheurs de fonction, surveillance continue des vulnérabilités et de l'état de conformité, visibilité sur tous les services Amazon et AWS connectés (CloudWatch, Elastic Cloud Compute (Amazon EC2®)...) et DynamoDB®, etc. Protégez les fonctions AWS Lambda en cours d'exécution contre les activités indésirables dans les processus, sur le réseau ou dans les systèmes de fichiers.
- **Sécurité CI/CD** – Intégrez la sécurité aux workflows CI/CD. Définissez des seuils de vulnérabilité granulaires pour signaler/bloquer les fonctions vulnérables ou déclencher des alertes/appliquer des politiques de conformité.

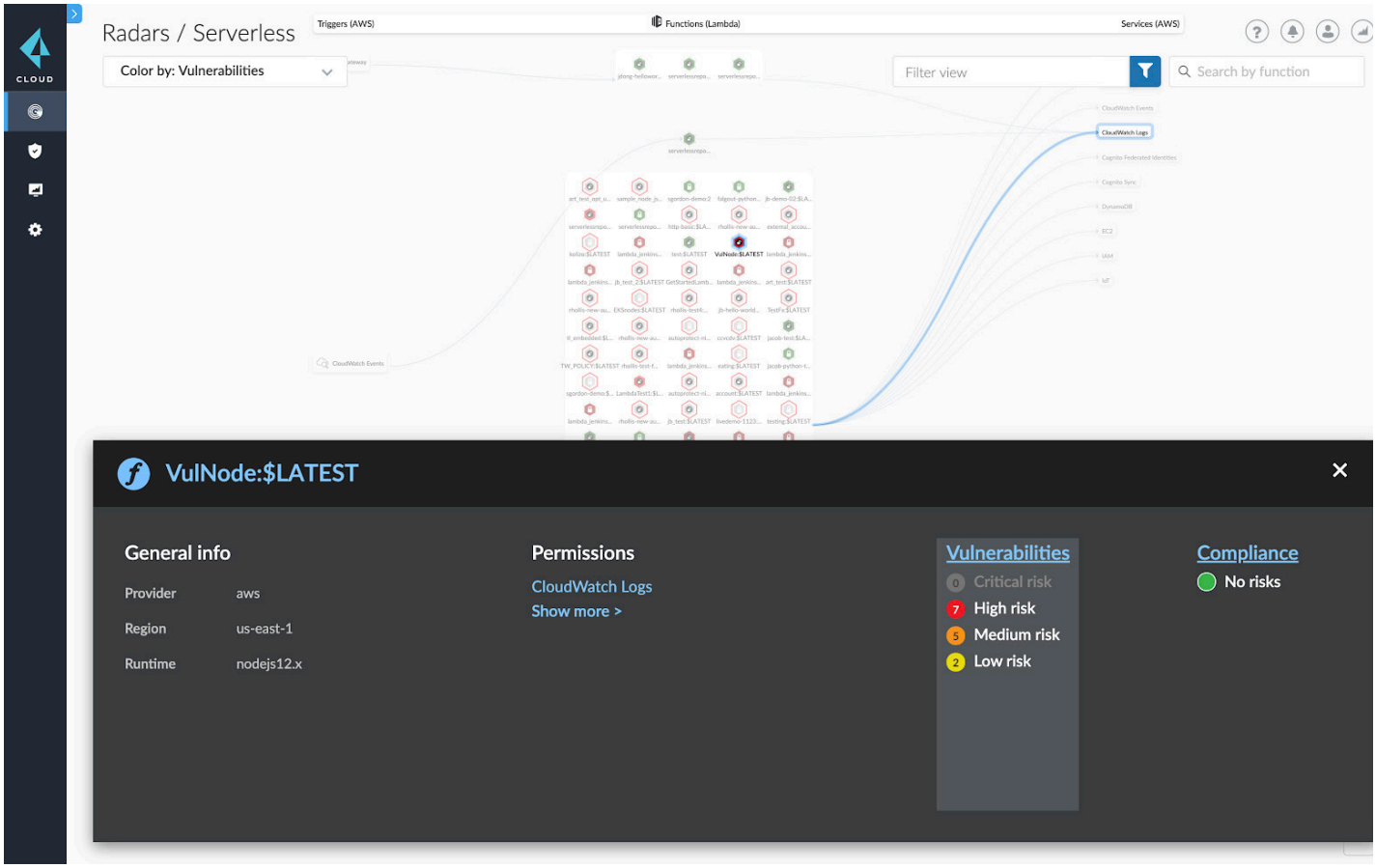

Figure 3 : Sécurité des systèmes sans serveur

Sécurité des API et des applications web

Prisma Cloud Web Application and API Security protège les environnements cloud publics et privés contre les menaces sur la couche L7 et le top 10 de l'OWASP. Au menu :

- **Protection contre les menaces du top 10 de l'OWASP** – Signalez ou anticipez les principaux scénarios d'attaque du top 10 de l'OWASP (injections SQL, scripts intersites (XSS), protection Shellshock, attaques par force brute, etc.).
- **Protection des API** – Identifiez les API protégées et non protégées, puis configurez des règles et actions de sécurité en toute simplicité.
- **Protection du chargement des fichiers** – Définissez des alertes ou appliquez des restrictions de chargement (upload) en fonction de l'extension du fichier et du contenu détecté. Des contrôles granulaires permettent d'autoriser, d'alerter ou de bloquer des formats de fichiers spécifiques (audio, archives compressées, documents, images, vidéos, etc.).
- **Contrôles d'accès géosensibles** – Empêchez les accès web de clients provenant d'adresses IP, de réseaux ou de pays spécifiques.
- **Protection des applications web basée sur les en-têtes HTTP** – Définissez des critères permettant d'autoriser ou de refuser l'accès aux applications web en fonction de noms ou d'en-têtes HTTP.

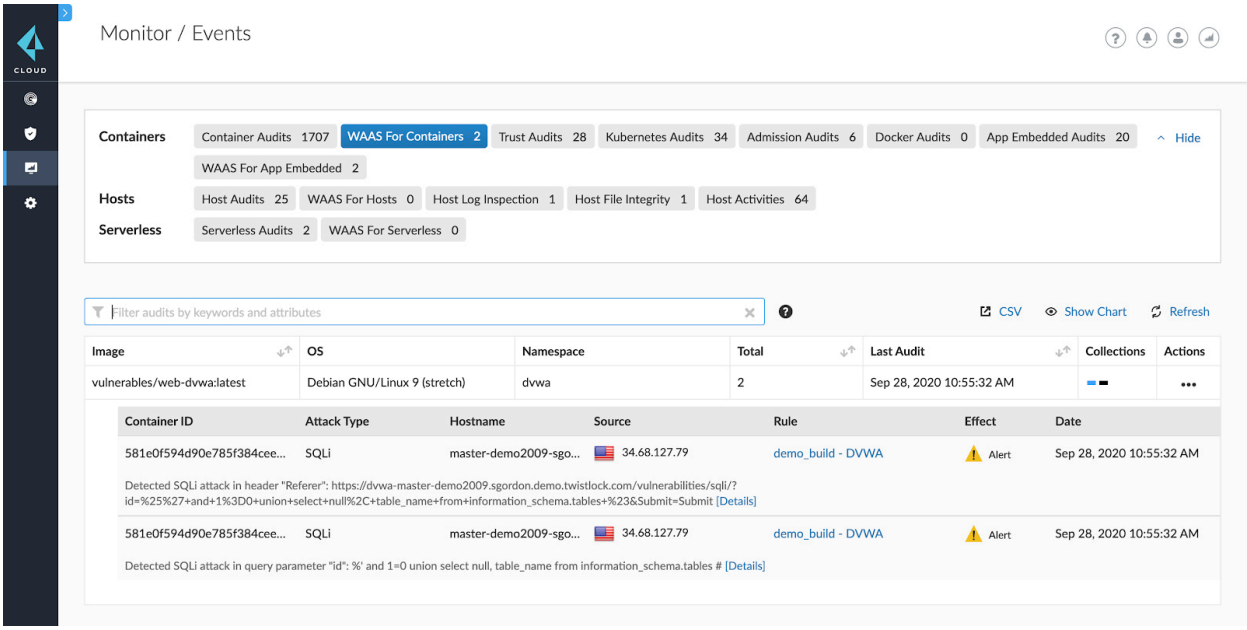

Figure 4 : Sécurité des API et des applications web

Prisma Cloud est la plateforme de sécurité cloud-native la plus complète du marché. Sa mission : assurer la protection et la mise en conformité de vos applications, données et technologies cloud-native tout au long du cycle de développement sur vos environnements cloud hybrides et multi-cloud. Au lieu de s'assujettir aux contraintes de sécurité des architectures du cloud-native, l'approche intégrée de Prisma Cloud les élimine et brise les silos de sécurité opérationnelle tout au long du cycle de vie des applications. Vous pouvez ainsi évoluer vers une approche DevSecOps et réagir plus rapidement aux besoins de sécurité changeants des architectures cloud-native.

Pour en savoir plus, rendez-vous sur notre site web ou visionnez une démo.

« Prisma Cloud aide notre entreprise à adopter le concept de DevSecOps pour évaluer la sécurité à chaque étape du développement. Si une vulnérabilité ou une faille est découverte, nous la corrigeons avant la mise en production. »

– Nicola Mutti, Responsable sécurité, Cuebiq

Lire l'étude de cas complète

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr